Report on the operation and effectiveness of the COVIDSafe application - DRAFT

26 April 2020 to 31 July 2021

Authored by:
Richard Nelson
Vanessa Teague
Geoffrey Huntley

August 2021

Table of Contents

Authors' Forward

On the 29th of July, 2021, the Australian Government released a report[1] on the effectiveness of the COVIDSafe application. The report lacks a deep discussion of changes made throughout the app's development which heavily impacted efficacy, and fails to disclose key information such as the number of active users of the application. This is in stark contrast to the peer reviewed article in Nature[2] which examines in detail the epidemiological impact of the NHS application developed in the UK. The Australian Government's report does disclose information on the number of close contacts and encounter uploads, which are also used in this document.

The release of COVIDSafe in April 2020 garnered intense interest and scrutiny from the tech community. The authors of this document are among technical experts who took interest in the ongoing development of the COVIDSafe application, with demonstrated submissions[3] to the DTA which had significant positive impact on the security, privacy and effectiveness of the iOS and Android COVIDSafe applications.

It is important to discuss both the successes and shortcomings of the development process and outcomes of COVIDSafe. At the beginning of the COVID-19 outbreak, there were many unknowns, with different approaches in technological aids to contact tracing being undertaken worldwide. The Australian Government chose throughout the evolving technical landscape to continue with their centralised model of contact tracing with COVIDSafe and continued to diverge from expert implementation of the Exposure Notification Framework by Apple and Google, despite suggestions from the Government that there would be early take up of this technology.

Purpose of this report

This report uses factual information presented in the Government's report, along with known technical capabilities and limitations of the application in order to make recommendations for future work. We wish to inform the reader of decisions and statements made which impacted the effectiveness, privacy and security aspects of the

---

1 https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/bc7d2dd0-da92-4238-abfa-19589961f1c6/upload_pdf/D21-1478556%20%20FINAL%20-%20Report%20on%20the%20operation%20and%20effectiveness%20of%20COVIDSafe%20and%20the%20National%20COVIDSafe%20Data%20Store.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/bc7d2dd0-da92-4238-abfa-19589961f1c6%22

2 https://www.nature.com/articles/s41586-021-03606-z

3 https://github.com/vteague/contactTracing/blob/master/blog/2020-07-07IssueSummary.md

COVIDSafe application, and negatively affected the community perception of the application.

We also compare more thoroughly with other technical solutions used globally, in particular Google and Apple's collaboration on their Exposure Notification Framework (GAEN).

The intended audience of this report are people who want to have an understanding of the history and issues that the COVIDSafe app faced with regards to functionality, security and privacy, and those who wish to learn from these challenges that the development of the COVIDSafe application faced.

We also draw on this experience to make recommendations for better tech development and decision making, not just for COVIDSafe but for other government tech projects. There is a double cost when a project like this doesn't work: the expense, and the opportunity cost of failing to produce a solution that might have solved an important problem. We conclude by explaining how we think future projects could do better.

Launch of COVIDSafe

COVIDSafe was launched on the 26th of April, 2020, as a technical aid to contact tracing. The iOS and Android applications were built on Singapore's OpenTrace[4] code from their TraceTogether application. The Government stated in May that the application had been downloaded more than 4 million times, a good initial response. Well-known Australian technology and security experts, such as Troy Hunt, gave recommendations to the public to download and use the application.

Prior to launching the application, the source code was reviewed by "government security agencies, academics and industry specialists". It is unclear exactly which groups or individuals these were, what advice was given at the time, and whether the review related to the mobile applications, and/or the National COVIDSafe Data Store (NCDS).

Early on, it was clear that there were security, privacy, and functional issues with COVIDSafe. With a quick-to-market application, it's expected that there might be imperfections and improvements to be made, but the initial response from the DTA to

[4] https://github.com/opentrace-community

some of these issues was slow. After a number of these issues had been reported, an update to the application with a visual redesign was released, without fixes to any of the issues posed.

There was initially no clear process for reporting security vulnerabilities. Without a Vulnerability Disclosure Policy, in some instances researchers became frustrated with a lack of response and publicised issues in ways that may have contributed to driving down public perception. A security disclosure method was added shortly after, and the DTA began publishing limited security advisories on GitHub.

Operation of the app

COVIDSafe is a standard application as installed from Google Play and Apple's App Store, which runs on iOS and Android phones. Standard applications have some restrictions, particularly on iOS, where it is not guaranteed that an application can reliably keep running tasks when not actively in use, even with background modes enabled.

The app uses devices' Bluetooth functionality to discover and connect to other users who are running the application. Once connected, depending on the version of the application, it either sends or exchanges an identifier. This record is called an "encounter", and is stored in the application database on the device for 21 days, regardless of whether it's part of a set of encounters making up 15 minutes at 1.5m or not. The application regularly removes encounters older than 21 days. Encounters are available to extract from devices by users with enough technical knowledge, but the contents of the encounters are encrypted. Early versions of the application did not have encrypted encounters, so although the identifiers were anonymous, metadata of the encounters was available.

If a person who has tested positive to COVID-19 consents to upload app data, the application uploads the encounter log in its entirety.

The identifiers used in these exchanges are provided to the application by a server, have an expiry, and are regularly updated.

The use of Bluetooth in this way, as designed by Singapore's TraceTogether team, is novel. Bluetooth devices typically do not advertise their presence indefinitely as well as allowing connections from other devices without at least an initial (possibly implicit) form of user approval. Nor do they typically act in these peripheral (listening) and

central (scanning and initiating connection) modes indefinitely. Critically, there is no way for the application to verify that another device connecting to it is another device running the COVIDSafe application, and not a potentially malicious device pretending to be the COVIDSafe app. This vastly increases the risk of implementation bugs, security and privacy issues, all of which eventuated with serious impact.

The Google-Apple Exposure Notification framework

Around the same time that COVIDSafe was being developed, Apple and Google developed and released a framework specifically designed to address the same problem. In many ways, the Google-Apple Exposure Notification (GAEN) framework is similar to OpenTrace: it works by using Bluetooth messages between phones and attempts to measure signal strength and duration as a proxy for infection probability. However, the information flow is completely different: users do not keep a list of contacts and upload them to the government. Instead, they detect for themselves, on their own device, whether any of their anonymised contacts has tested positive. The authorities do not necessarily receive information about who has been exposed, and the system does not convey who exposed whom.

The GAEN protocol is therefore inherently more privacy-preserving than COVIDSafe's centralised model, though its privacy guarantees are not perfect. For example, it is often not difficult to infer which of your contacts has contracted COVID19. Maintaining the secrecy of who infected whom is good for privacy, but unhelpful for epidemiological studies. However, GAEN does not prevent public health authorities from being notified when the app detects an exposure - this is not inherent to the protocol, but is allowed on an opt-in basis and is used by several countries.

It is also more efficient. It does not make connections between devices, nor does it have app-level restrictions to modes of operation. The GAEN framework's bluetooth broadcast is advertised as non-connectable, and their "temporary exposure keys" are included as part of the broadcast payload, making connections unnecessary. This passive, connectionless method also has the advantage of using fewer resources and therefore has less impact on battery usage.

Privacy

The COVIDSafe application was designed around solid privacy principles, assuming a central data-gathering model. Parliament made amendments to the *Privacy Act 1988* which ensured that data collected by the application could only be used for the

purposes of contact tracing, and that it prohibited anyone from requiring that the COVIDSafe application be used.

The application's protocol for discovery and data exchange was designed in a way to ensure anonymity on encounter exchanges, and to mitigate tracking users around locations. This is extremely important for reasons ranging from not allowing businesses to track customers and collect behavioural analytics, to making the tracking of domestic violence victims or other at-risk people infeasible.

Contacts were uploaded only when a user tested positive for COVID. In this sense, COVIDSafe's design was much better for privacy than state government QR-code-based check-in apps, which upload check-in data immediately.

Unfortunately, the hurried release of the application and lack of implementation by or collaboration with experts who understand Bluetooth at a low level, meant that there were serious privacy issues with the implementation. Although the app was designed with privacy in mind, there was very little testing or verification in this area. This resulted in bugs ranging from phone model and name being constantly exposed and unique identifiers being available to track over time, to undetectable, permanent long-term tracking of iOS and Android devices and attackers being able to control devices remotely.

These bugs could mostly have been avoided by using the Exposure Notification Framework provided by Apple and Google, two companies which understand both the range of users' threat models with regard to exposed network protocols, and who have the vast technical expertise required to solve them.

Security

COVIDSafe is designed and implemented to ensure that the data exchanged by devices and stored on AWS servers is encrypted and therefore not vulnerable to data disclosure, especially by a user who is able to gain access to COVIDSafe data on their device. The end to end encryption of the data ensures this, and only the NCDS can decrypt this data. To date, there have been no known incidents of users decrypting data or directly identifying users in encounters.

Versions of the application up to 1.0.18 did not encrypt payload data, meaning that encounter metadata (RSSI, phone model, date/time, temporary identifier) could be

extracted by users. The temporary identifiers are meaningless to the user, so users extracting this data could not identify other users in encounters directly.

A number of security related bugs were found and reported by the tech community, and the DTA started raising Security[5] Advisories[6] on GitHub. However, only a small subset of security vulnerabilities were released as advisories by the DTA. Issues such as CVE-2020-12856[7], which was assigned a CVSS 3 score of 9.8 and deemed “Critical”, and allowed for silent pairing of Android devices and then allowed an attacker to switch profile and remotely control the device, were not included.

In December 2020, COVIDSafe was updated with integration of the “Herald” protocol. The DTA made the statement that “Cyber security experts have undertaken a comprehensive security audit of Herald’s integration into COVIDSafe”. Despite this, the same class of bug was found on both the iOS and Android versions of the application that had surfaced previously, allowing an attacker to remotely (within Bluetooth distance) disable the application. Security Advisories for these bugs were not released by the DTA.

Software security is challenging. However, decisions around design of the COVIDSafe protocol increased the risk of potential security problems. Additionally, software security testing with regards to Bluetooth connectivity was minimal, and security bugs resurfaced from version to version. These would not have occurred if test cases and security audits learnt from previous issues.

The complexity of Bluetooth protocols and therefore attack surface can be severely reduced by using GAEN framework. It is connectionless, hides details of Bluetooth scanning and records from the application, and has been implemented by companies who are experts in cyber security. This would allow COVIDSafe developers to focus on user experience and would have minimised resulting security vulnerabilities.

Effectiveness of the app

When COVIDSafe was first released in late April 2020, there was confusion as to whether or not any improvements had been made on the publicised limitation of TraceTogether; that the iOS application required users to keep the app open and in the foreground for encounters to be recorded. It was stated that improvements had been

[5] https://github.com/AU-COVIDSafe/mobile-android/security/advisories
[6] https://github.com/AU-COVIDSafe/mobile-ios/security/advisories
[7] https://github.com/alwentiu/COVIDSafe-CVE-2020-12856

made in this area, which turned out to be incorrect. Alarmingly, the statements that were being made by both the TraceTogether team and the DTA contradicted Apple's documentation on how iOS applications could continue to have Bluetooth effective while an application is running in the background.

It was quickly shown[8] that the limitations of COVIDSafe running in the background on iOS had been inherited from Singapore's TraceTogether application, and it should not have required users to keep the app open in the foreground.

At a Senate committee hearing investigating Australia's coronavirus response, the then DTA chief executive officer Mr Randall Brugeaud stated:

"The quality of the Bluetooth connectivity for phones that have the app installed and running in the foreground is very good, and it progressively deteriorates and the quality of the connection is not as good as you get to a point where the phone is locked and the app is running in the background"

This behaviour was at the time largely blamed on limitations that Apple set on background apps on iOS:

"Apple could fix this tomorrow, they could actually ensure that the Bluetooth strength was at the highest possible level tomorrow for applications built in a sovereign framework and we're working with Apple constructively on this." -- Minister for Government Services Stuart Robert MP

Ultimately, several bugs in the COVIDSafe app itself - which were investigated and reported by the community - explained this undesired behaviour, and they were subsequently fixed in updates to COVIDSafe without requiring Apple to modify the behaviour of iOS, though smaller underlying limitations remain.

- iPhone app only functions in the foreground[9]
- iPhone app cannot continue to function when locked[10]
- iPhone app prevents new connections after 100 exchanges[11]

---

[8] https://medium.com/@wabz/the-broken-covidsafe-ios-application-c652d0a462c4

[9] https://medium.com/@wabz/the-broken-covidsafe-ios-application-c652d0a462c4

[10] https://docs.google.com/document/d/1dsSxC48cJ91X17PoOybpun1U163YDxxL0CDk3kmAHvY/preview

[11] https://github.com/vteague/contactTracing/blob/master/blog/2020-07-07IssueSummary.md#13-iphone-app-prevents-new-connections-after-100-exchanges

- The above issue was reintroduced with Herald integration

The 3rd issue was not fixed until August 2020. This bug also prevented iOS devices from correctly communicating with other devices, such as diabetes monitoring apps[12], heart rate monitors, workplace entry gates, motor vehicles, Apple Watch, headphones, game controllers, and other medical devices.

There were also bugs with the implementation of the encryption algorithms. An issue with payload size[13] was found on iOS, which reduced the reliability of encounter logging by corrupting the exchanged data. This bug could have been found by automated integration testing or field testing.

In December 2020, the COVIDSafe app switched to "Herald," a new implementation of a Bluetooth-based encounter exchanging. Herald uses the same Bluetooth connection method that COVIDSafe traditionally used, but contains a number of workarounds to keep Bluetooth scanning and connections persistent. However, the underlying issues remain. It was immediately shown that two locked iPhones will still not detect each other until other devices are in the picture. It is still unclear that the application will continue to function in cases where the operating system may have stopped it.

The DTA asked the community for feedback on the implementation of the Herald protocol prior to releasing this version of COVIDSafe to the public. Members of the tech community, composed of experts in the fields of mobile application development, cryptography, and Bluetooth, reviewed the Herald implementation and continued to implore the Government to switch to the Exposure Notification Framework. Security and functional bugs were again found and reported. The workarounds used in Herald reduced public perception of the application. For example, it introduced a requirement for the iOS application to request location permission, something that should not be required where location isn't used, and indeed was not prior to Herald. Requesting permissions for anything other than intended use is also against App Store Review Guidelines, and could get the app removed from the store. Additionally, the prompt requesting permission for location tells the user that location is used for "relevant COVID-19 alerts", which is clearly untrue as there is no code for such a mechanism.

---

12 https://www.smh.com.au/technology/covidsafe-may-interfere-with-diabetes-monitoring-apps-20200501-p54oyd.html

13 https://github.com/vteague/contactTracing/blob/master/blog/2020-06-19IssueswithCOVIDSafesNewEncryptionScheme.md

In the 6 month reporting period (from the 16th of November 2020 to the 16th of May 2021), 44 users uploaded COVIDSafe data. 248 unique close contacts came out of that, which equates to ~5.6 contacts per upload. The UK's NHS app, which uses the Exposure Notification Framework, had 4.4 contacts notified per positive user who consented to have their contacts traced. However, the Exposure Notification Framework captures 14 days worth of data, compared to COVIDSafe's 21. Normalising these, the NHS app had 0.314 contacts per day, and COVIDSafe a slightly lower 0.26. While interesting, these numbers are difficult to compare directly, as the DTA have not released the number of active users of COVIDSafe.

In the Australian government's official report on COVIDSafe, the entire section on Effectiveness is completely redacted.

Engagement with the technical community

A public code repository is more than most commonwealth government entities usually make available (neither myGovID nor the Senate count has any available source code). This was a welcome development, which allowed for detailed analysis and numerous bug-fixes that would have been much harder with a closed-source system. However, there were artificial limitations that prevented this tool being as effective as it could have been.

- The conditions were unreasonable, for example requiring reviewers to be "responsible for any costs of third party claims associated with my access to the App Code." This strongly disincentivised participation.
- Rather than being shown as it was developed, the code was pasted into the public repository, often some days after the equivalent version had shipped. This made it impossible to find bugs before they affected users. For example, a public review of the code change to fix the bug causing iPhones to reach a maximum number of connections would have found that it was not sufficient.
- The server code stayed hidden - there were some hints that this was a continuing source of serious functionality problems, which the open community was unable to address. It was particularly unfortunate that the secrecy of this code was often linked in public statements to the privacy of users,[14] as if keeping it secret would substitute for solving security problems.

Security disclosures were slow to be set up, but are now set up much better, with obvious instructions, an email address, and a public key for encrypting the information. This setup should be retained for future projects.

[14] https://www.innovationaus.com/app-server-code-needed-for-transparency/

A chance to fix problems after the fact is welcome, but it would have been a lot better if we could have influenced design decisions in advance. Most of us could have explained, in advance, that

- GAEN was likely to work a lot better than a centralised BLE-based model, and
- Herald wasn't going to fix perceived or real technical issues.

In summary, engagement with the technical community was better than most other Australian government IT projects, but it is very unfortunate for Australia that the bar is so low. Earlier and deeper engagement might have produced much better results for much less cost.

Communication with the public

It is commendable that the application was released within a matter of weeks, and understandable that the Government wanted to react quickly to implement technological measures to slow the spread of COVID-19. However, flaws with early versions of the application caused a sharp dive in public perception, from which it did not recover, despite efforts from the tech community to assist with and guide direction. It should have been clear early on that a design using Bluetooth connections opened COVIDSafe up to a swathe of privacy, security, and functional problems, and that the DTA and its engaged partners were not well-equipped to find or solve them.

Commentary from the DTA and politicians on switching to the framework provided by Google and Apple was largely misleading or incorrect. A spokesperson for Government Services Minister Stuart Robert's office stated: "The current Apple and Google tracing platforms are structured very differently. They rely on the individual who tests positive to initiate sending the alert to the close contacts, and those people reacting to automated notifications, isolating and getting tested."

"Public health officials won't have access to that information, which will reside with Google and Apple. This is high risk. People may ignore the information and that will lead to the further spread of the virus."

There were multiple misleading statements made here. The first is the claim that Apple and Google would have access to information about who tested positive and who is notified of exposure. In fact, as described above, the GAEN protocol is carefully designed so that exposure detection occurs on the person's device and does not need

to be relayed through any authority. The Exposure Notification Framework does not tell Apple or Google who is being notified of covid exposure.

It is also not true that “public health officials won’t have access to that information.” Exposure notifications can still only be triggered by a health authority publishing the key of a positive case. Although GAEN does not require that the app receiving the exposure alert notify public health officials, the app can indeed automatically notify public health officials, and can also include contact information. Contact information is permitted only on an opt-in basis and does not have to identify the source of the exposure, though the app could strongly recommend the user provide information, particularly at notification time. The public health officials could then follow up with the exposed person, answering their questions and instructing them to isolate, exactly as they now do in Australia. At the time this statement was made, there were other applications around the world that worked in this way, including Ireland’s COVID Tracker app, England and Wales’ NHS COVID-19 app and New Zealand’s Covid Tracer app.

The advantage of such a design is that close and casual contacts can be notified as soon as a confirmed positive case is found. This removes the bottleneck of manual contact tracing, and when health officials do follow up the cases can already be isolating.

Conclusion

Initial public takeup of the application was good, reaching more than 4 million downloads by May 2020. However, it became clear that issues suffered by the COVIDSafe application drastically reduced public perception and therefore reduced the number of people downloading, installing and using COVIDSafe. When major issues were fixed (e.g. background behaviour on iOS), marketing was somewhat muted, resulting in the continued perception (real or not) that the application did not function well.

COVIDSafe efficacy data from the DTA continues to be opaque. Without knowing the number of active users, it is still difficult to determine how well the application has been working. In contrast, the UK’s NHS, which abandoned early efforts on connection based Bluetooth methods and implemented Apple and Google’s Exposure Notification Framework, have published peer reviewed research on the epidemiological impact of their application.

Almost all of the serious security bugs, privacy issues, and bugs affecting efficacy that were present could have all been avoided by using the Exposure Notification Framework, keeping public perception high.

We recommend that the Government implement the Exposure Notification framework. A quick win would be to implement Exposure Notification Express as a first step.

The pandemic is unlikely to disappear soon, and it is still worth pursuing a bluetooth-based exposure notification system that works. Using the Exposure Notification framework, which is a secure, privacy-based approach that is known to work, has many advantages over COVIDSafe's approach, and the supposed downsides have been both misunderstood and overstated.

Australia needs to learn to build public-sector tech that works and earns public trust. The Australian government should build and expand on its program of source code availability, making more of our technology more easily accessible to Australians for analysis and improvement. This both improves the technology and builds public trust. Incorporating technical expertise earlier into the design phase would improve high-level decision making.

Resources

Australian Government's Report on the operation and effectiveness of COVIDSafe and the National COVIDSafe Data Store[15]

COVIDSafe issues found by the tech community[16]

Fools rush in where angels fear to tread - why Herald won't be ready by Christmas[17]

---

15 https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/bc7d2dd0-da92-4238-abfa-19589961f1c6/upload_pdf/D21-1478556%20%20FINAL%20-%20Report%20on%20the%20operation%20and%20effectiveness%20of%20COVIDSafe%20and%20the%20National%20COVIDSafe%20Data%20Store.pdf;fileType=application%2Fpdf#search=%22publications/tabledpapers/bc7d2dd0-da92-4238-abfa-19589961f1c6%22

16 https://github.com/vteague/contactTracing/blob/master/blog/2020-07-07IssueSummary.md#covidsafe-issues-found-by-the-tech-community

17 https://github.com/vteague/contactTracing/blob/master/blog/2020-12-07COVIDSafeHerald.md#fools-rush-in-where-angels-fear-to-tread---why-herald-wont-be-ready-by-christmas